UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,920	03/09/2004	Kenneth L. Levy	P0951	3347

23735 7590 07/01/2008

DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008

EXAMINER	
STANLEY, MARK P	

ART UNIT	PAPER NUMBER
2623	

MAIL DATE	DELIVERY MODE
07/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/797,920	LEVY, KENNETH L.	
	Examiner	Art Unit	
	MARK P. STANLEY	2623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

Applicant argues that Roese does not teach forming an IP packet where the header data includes additional data defining restrictions. Examiner respectfully disagrees, Roese teaches the use of a tag for defining boundaries as described in paragraph 115, where paragraph 116 states "the server generating a data packet to transport the data over the network can add this tag while generating the data and/or packet", where Roese states in paragraph 117 "a device within system 100 and/or the data itself determines (step 625) whether the data is outside the permitted location(s)" and paragraph 98 teaches the device limiting the packet transmission in system 100 of Fig. 1 being a firewall, where paragraph 98 states "firewalls are primarily computer programs designed to analyze packets and, from that analysis, make a determination as to whether packet transmission into or out of the network is permitted". Therefore, data added to the packet based on the tag during generation of the packet includes the given additional data, where the firewall may analyze the body or header of the packet, it is understood that both placing additional data in the header and/or the packet is taught such that the firewall has means to properly analyze the additional data of the packet to determine restrictions.

Applicant argues that Roese does not teach two states indicating certain restrictions. Examiner respectfully disagrees, as stated above the additional data in the packet as a result of the tag provides boundary restrictions, and the additional data does have two states indicating certain restrictions, paragraph 115 of Roese states "defined boundaries (e.g., a present device, a room, ..." where a first state being the additional data prohibiting the transmissions of the copy of data in the packet to certain destinations and a second state being the additional data prohibiting transmissions to any destination that is outside the present device meaning transmissions to any location from the present device is prohibited

Applicant argues that Roese does not teach limitations "concerning physical location and proximity" or restriction transmission based on "destination address specified in the packet header". Examiner respectfully disagrees, where claim 4 states "forming an IP packet" with corresponding limitations and claim 11 states "receiving an IP packet" with corresponding limitations. As described above, Roese teaches both generating an IP packet with additional data conveying restriction information at a first device location (Fig. 1, item 104), and receiving and analyzing the generated IP packet at a second device location (Fig. 1, item 114) such as a firewall. Where at the second device it is determined as stated in paragraph 117 "if the data is going to be routed in the next hop to a location that is outside the permitted location(s)" thus the destination of the packet determined in the packet header is analyzed and further, the permitted location may be as stated in paragraph 115 the present device being that the

data is not permitted transmission at all outside the first device. Therefore, the packet received at the second device determines according to the additional data that the packet is in a first state being that it is prohibited from any transmission outside the first device and the second device accordingly prohibits further transmission. On the other hand, when the second device receives the packet and determines according to the additional data that the packet is in a second state being that transmission is allowed but also prohibited from transmission to devices not within a set region ([0115]), the second device will accordingly prohibit further transmission when it is determined the next hop for the packet to be routed to is not a physical location within a specified region.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 4, 7-9, 11, and 13-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Roese et al. (US 2003/0217122 A1 hereinafter Roese).

Regarding claim 4, Roese discloses "a method of data processing that includes forming an IP packet having header data and body data, wherein the header data includes a first destination address, the method comprising:

forming said header data to additionally include additional data specifying whether it is permissible to send a copy of data in the packet to a second destination address, wherein the additional data has at least two states, respectively indicating: ([0115]-[0117], a tag is used for generating a packet with additional data for placing transmission restrictions as described above)

(a) it is not permissible to send a copy of data in the packet to any second destination address; or" ([0115], Fig. 1, where paragraph [0115] of Roese states 'defined boundaries (e.g., a present device, a room, ...' where the tag incorporates both states being that the tag may prohibit transmissions to certain destinations or prohibit transmissions to any destination that is outside present device meaning transmissions to any location from the present device is prohibited)

"(b) it is not permissible to send a copy of data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address" ([0115]-[0118], Fig. 6, describes preventing the data from being sent to any other destination, [0117] describes selectively preventing data from being sent to any destination outside of a set domain, [0115] describes a device may not transmit data to any other destination outside a domain, where no device may be authorized to receive the content no matter the device location).

"wherein said domain comprises networked devices associated with a single family" ([0115], any devices that belong to a single entity such as a campus regardless of who uses the devices belonging to the single entity constitutes as a domain of network devices associated with a single family where the restrictions on the exchanging the content may be limited to within the domain of the single family such as any network devices within a campus)

Regarding claim 7, Roese discloses "the method of claim 4 wherein a device associated with the first destination address has a first physical location and a device associated with the second destination address has a second physical location, and the additional data includes a field signaling that copying of data in said packet to said second destination address should be:

(a) permitted if the second physical location is physically proximate to the first physical location; and

(b) prohibited if the second physical location is physically remote from the first physical location" ([0100]-[0103] describes the location limitation being a physical location limitation)

Regarding claim 8, Roese discloses "the method of claim 7 wherein the first and second destination addresses are within a common domain" ([0100]-[0103], Fig. 1, Fig. 8, where the first and second destination devices can be within a common domain).

Regarding claim 9, Roese discloses "the method of claim 7 wherein the first and second destination addresses both correspond to network devices associated with a single family" ([0100]-[0103], Fig. 1, Fig. 8, network devices allowed within the network may be limited to a single family).

Regarding claim 11, Roese discloses "a method of data processing that includes receiving an IP packet having header data and body data, wherein the header data includes a first destination address, the first destination address corresponding to a device at a first physical location proximate to where said method is practiced, the method comprising interpreting additional data in the header of said packet as specifying whether it is permissible to send a copy of data in the packet to a second destination address, wherein:" (Roese teaches both generating an IP packet with additional data conveying restriction information at a first device location, Fig. 1 item 104, as described in claim 4 above, and receiving and analyzing the generated IP packet at a second device location, Fig. 1 item 114, such as a firewall as described in the response to arguments above. Where at the second device it is determined as stated in paragraph 117 "if the data is going to be routed in the next hop to a location that is outside the permitted location(s)" thus the destination of the packet determined in the packet header is analyzed for determining hops and enforcing restrictions on the packet)

"(a) if the additional data has a first state, prohibiting transmission of a copy of data in the packet to any second destination address; and" ([0115]-

[0117], the packet received at the second device determines according to the additional data that the packet is in a first state being that it is prohibited from any transmission outside the first device and the second device accordingly prohibits further transmission)

"(b) if the additional data has a second state, prohibiting transmission of a copy of data in the packet to any second destination address other than a second destination address within a domain that also includes the first destination address" ([0115]-[0117], when the second device receives the packet and determines according to the additional data that the packet is in a second state being that transmission is allowed but also prohibited from transmission to devices not within a set region, the second device will accordingly prohibit further transmission when it is determined the next hop for the packet to be routed to is not a physical location within a specified region, where the destination of the packet determined in the packet header is a determining factor in the hops).

Regarding claim 13, the claim is rejected for the same reasons as claim 4 above.

Regarding claim 14, the claim is rejected for the same reasons as claim 7 above.

Regarding claim 15, the claim is rejected for the same reasons as claim 8 above.

Regarding claim 16, the claim is rejected for the same reasons as claim 9 above.

Regarding claim 17, Roese discloses "the method of claim 14 wherein the method includes determining whether the second physical location is physically remote from the first physically location by reference to whether the second destination address is served by a common firewall with the first destination address ([0098] describes combining the use of a firewall with the physical locations of the devices, where it states a firewall makes determination of packets into and out of a network).

2. Claims 19-21 and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by Levy (US 2001/0044899 hereinafter '899).

Regarding claim 19, '899 discloses "a method wherein content is divided and collectively represented by plural packets of data, each packet having first and second portions," ([0035] packetizing the content into a header portion with watermark commands based on the watermark payload in the body portion) "the first portion of each packet including a divided part of the content, the method including obtaining an identifier of said content, and including said content identifier in the second portion of each packet" (the body portion including the watermark payload is the first portion, the header portion including watermark commands is the second portion).

Regarding claim 20, '899 discloses "the method of claim 19 wherein said obtaining includes examining a previous representation of said content that has an identifier associated therewith" ([0022]-[0023] states detecting a watermark and extracting content identification information used in transmarking for preservation of the watermark)

Regarding claim 21, '899 discloses "the method of claim 19 wherein the packets comprise IP packets," ([0039] streaming Internet broadcasts utilize TCP/IP) "each having a body portion as said first portion, and a header portion as said second portion, said header portion including address information in addition to said content identifier" ([0035] packetizing the content into a header portion with watermark commands based on the watermark payload in the body portion).

Regarding claim 24, '899 discloses "the method of claim 19 that further includes reading the content identifier from the second portion of one of said packets to identify content represented by data in the first portion" ([0035], a packet header containing watermark commands based on the watermark payload).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 10, 18, 25-26, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese et al. (US 2003/0217122 A1 hereinafter Roese) in view of Levy (US 2001/0044899 hereinafter '899).

Regarding claim 1, Roese discloses "a method of enforcing geographical restrictions on content redistribution in a TCP/IP network, an improvement comprising defining a geographical boundary across which certain content does not pass, wherein said boundary is defined--at least in part--by a hardware firewall device" ([0098], [0115]-[0118], Fig. 6, where [0098] describes the use of firewalls with devices sending and receiving content information, [0117] describes preventing the data from being transmitted at the point of transmission or at the point of reception depending on assigned restrictions of the data).

"determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to flag bits included in the header of said packet" ([0115]-[0118], Fig. 6, where step 620 in Fig. 6 is where data being transmitted is tagged with information about a boundary restriction, and [0116] describes the tagged information being conveyed in the data packets being transmitted such that a device receiving the packet may appropriately restrict the packet upon analyzing).

But, while Roese states that a system determines the location sensitivity of data to be transferred and placing additional data in a generated packet to

identify restriction information at receiving devices ([0116]), Roese does not explicitly state placing the additional data as a packet header containing flag bits being "related to the payload of a watermark in the content". However, '899 discloses transmarking video entertainment data to preserve the use of a video entertainment data digital "watermark in the content" when modifying the signal of the video entertainment data including packetizing the video entertainment data ([0012]-[0013], [0015], [0019]).

'899 teaches that a watermark is first detected ([0022]) in an original embodiment of the data and information such as copy control parameters and content identifiers are extracted ([0023]). Subsequently, the detected watermark signal may or may not be removed ([0026]), and a second watermark is then added based on the first detected watermark ([0029]) where the second watermark is adapted to work in the intended environment ([0033]) such as a packet-based communication channel, where a packet header with information pertaining to a watermark payload in each packet is generated ([0035]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of '899 for preserving watermarks of digital content during transmission in a packet-based communication channel via transmarking an initial digital watermark of the content into watermark payloads in each packet with additional data placed in each packet header based on the watermark payload with the teachings of Roese for modifying packets with additional data based on tags, such that the additional data may convey restriction information on the data in the packets for

devices to determine whether to prohibit or allow transmission of packets. One would have been motivated to do so to provide restriction on content as intended free from malicious user intervention by referring to a payload of a watermark in the body data to determine the usage rules in a packet header, where Roese seeks to provide secure restriction on usage of content and a watermark securely provides restriction information hidden from a user.

Regarding claims 10 and 18, Roese teaches the method of claim 4 and 11 as described above, but Roese does not explicitly state "wherein said additional data is related to the payload of a watermark encoded in the body data". However, placing header information containing flag bits related to a watermark has been analyzed as in claim 1 above.

Regarding claims 25-26 and 28, Roese teaches the use of a tag for defining boundaries as described in paragraph 115, where paragraph 116 states "the server generating a data packet to transport the data over the network can add this tag while generating the data and/or packet", Roese states in paragraph 117 "a device within system 100 and/or the data itself determines (step 625) whether the data is outside the permitted location(s)" and paragraph 98 teaches the device limiting the packet transmission in system 100 of Fig. 1 being a firewall, where paragraph 98 states "firewalls are primarily computer programs designed to analyze packets and, from that analysis, make a determination as to whether packet transmission into or out of the network is permitted". Therefore,

data added to the packet based on the tag during generation of the packet includes the given additional data, where the firewall may analyze the body or header of the packet received, it is understood that both placing additional data in the header and/or the packet is taught such that the firewall has means to properly analyze the additional data of the packet to determine restrictions.

But, Roese does not explicitly state "extracting restriction information from header data conveyed with the video entertainment" or "discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment" and "including data indicating said ascertained restriction information in header portions of each of said IP packets".

However, '899 discloses transmarking video entertainment data to be preserve the use of a video entertainment data digital watermark when modifying the signal of the video entertainment data including packetizing the video entertainment data ([0012]-[0013], [0015],[0019). '899 teaches that a watermark is first detected ([0022]) in an original embodiment of the data and information such as copy control parameters and content identifiers are extracted ([0023]). Subsequently, the detected watermark signal may or may not be removed ([0026]), and a second watermark is then added based on the first detected watermark ([0029]) where the second watermark is adapted to work in the intended environment ([0033]) such as a packet-based communication channel, where a packet header with information pertaining to a watermark payload in each packet is generated ([0035]). Additionally, '899 discloses converting a header of the video entertainment data into a watermark ([0016]) such that a

watermark payload and packet header pertain to the header of the video entertainment data.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of '899 for preserving watermark and header information of a video entertainment data by placing information pertaining to the watermark and header data into the packet header with the teachings of Roese for placing tag information into the header of the packet based on the data packetized to enforce geographical limitations on exchanging the data. One would have been motivated to do so to provide restriction on content as intended free from malicious user intervention by referring to a watermark in the data to determine the usage rules, where Roese seeks to provide secure restriction on usage of content and a watermark securely provides restriction information hidden from a user.

5. Claim 22-23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Levy et al. (US 2002/0186844 hereinafter '844).

Regarding claims 22-23, '899 discloses the method of claim 19 as described above, but does not explicitly state the use of a file allocation table with preserving content identifiers in each non-contiguous block. However, OFFICIAL NOTICE is taken that storing data as non-contiguous blocks onto a storage medium and association by an allocation table was well known and would have been obvious to try for the purpose of storing data onto a medium containing

enough space but only non-contiguous space due to prior storage of unrelated data blocks and further the use of a file allocation table for the proper reconstruction of the data blocks, and where '899 states preserving the watermark of the content in each packet when data is broken into non-contiguous blocks during packetization ([0035]), it would have been obvious to also preserve the watermark in each non-contiguous block when the data is broken into non-contiguous blocks and stored in a storage medium.

6. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roese et al. (US 2003/0217122 A1 hereinafter Roese) in view of Levy (US 2001/0044899 hereinafter '899) and in further view of Levy et al. (US 2002/0186844 hereinafter '844).

Regarding claim 27, Roese and '899 teach claim 25 as disclosed above, but do not explicitly teach obtaining restriction information from a remote repository. However, '844 states the use of obtaining a content identifier from a video entertainment data digital watermark using the content identifier to retrieve usage restrictions imposed on the video entertainment data from an external database ([0025]-[0026], Fig. 1). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of '844 for obtaining restriction information from a remote repository associated with the video entertainment data via a content identifier determined by the digital watermark with the teachings of Roese and '844 where restriction information based on data to be transmitted imposing geographical

limitations is placed in the header of a packet. One would have been motivated to do so to further improved the teachings of '844 for using a digital watermark embedded in video entertainment data whereby accessing restriction information pertaining to the digital watermark that may not have been entirely contained within the digital watermark so as to provide a option of updating of the restriction information a remote database.

Contacts

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARK P. STANLEY whose telephone number is (571)270-3757. The examiner can normally be reached on 8:00AM - 5:00PM Mon-Fri EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Beliveau can be reached on (571) 272-7343. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Mark P Stanley/
Examiner, Art Unit 2623

/Scott Beliveau/
Supervisory Patent Examiner, Art Unit 2623